

AMENDMENTS TO THE CLAIMS

Listing of claims:

This listing of claims replaces all prior versions and listings of claims in the application.

1. (Original) A recording device detachably attachable to a reproduction apparatus reproducing and outputting encrypted content data, for receiving and recording said encrypted content data therein, comprising:

a data input/output unit (1202) allowing external data communication;

a first storage unit (1412) receiving said encrypted content data from said data input/output unit for storage;

a user information hold unit (1530) holding first user ID data provided to identify a user of said recording device;

a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed; and

a control unit (1420) controlling an operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit.

2. (Original) The device of claim 1, wherein said control unit allows said user ID data to be changed when externally provided user information and said first user ID data match.

Amendment
Serial No. 10/069,113
Attorney Docket No. 020233

3. (Amended): The device of claim 2, wherein said control unit allows said protection information to be changed and said user ID data to be added ~~changed~~ when said user information hold unit does not have said first user ID data registered therein.

4. (Original) The device of claim 1, wherein:
said protection information memory unit includes a first protection information memory unit (1520) holding first protection information included in said protection information for restriction on access to said recording device itself; and
said control unit is driven by said first protection information to prohibit additionally recording new encrypted content data in said first storage unit.

5. (Original) The device of claim 1, wherein:
said protection information memory unit includes a first protection information memory unit holding first protection information included in said protection information for restriction on access to said recording device itself; and
said control unit is driven by said first protection information to prohibit erasing new encrypted content data in said first storage unit.

6. (Original) The device of claim 5, wherein:

said protection information memory unit further includes a second protection information memory unit (1540) holding second protection information included in said protection information for restriction on access for each said encrypted content data; and

said control unit is driven by said first and second protection information to prohibit erasing encrypted content data held in said first storage unit and corresponding to said second protection information.

7. (Original) The device of claim 1, wherein:

said protection information memory unit further includes a second protection information memory unit holding second protection information included in said protection information for restriction on access for each said encrypted content data; and

said control unit is driven by said second protection information to prohibit erasing encrypted content data held in said first storage unit and corresponding to said second protection information.

8. (Original) The device of claim 6, wherein when an external instruction is received to effect an operation to reproduce said encrypted content data, said control unit controls said first storage unit and is driven by said second protection information to prohibit providing said data input/output unit with encrypted content data held in said first storage unit.

9. (Original) The device of claim 8, wherein when externally provided user information and said first user ID data match said control unit controls said first storage unit and is driven by said second protection information to prohibit providing said data input/output unit with encrypted content data held in said first storage unit.

10. (Original) The device of claim 8, wherein when said user information hold unit does not have said first user ID data registered therein said control unit controls said first storage unit and is driven by said second protection information to prohibit providing said data input/output unit with encrypted content data held in said first storage unit.

11. (Previously Presented) The device of claim 6, wherein when externally provided user information and said first user ID data match said control unit permits rewriting at least one of said first and second protection information.

12. (Previously Presented) The device of claim 6, wherein when said user information hold unit does not have said first user ID data registered therein said control unit permits rewriting at least one of said first and second protection information.

13. (Original) The device of claim 1, further comprising a second storage unit (1500) holding license information data corresponding to said encrypted content data, respectively, and required for reproducing said encrypted content data, wherein when an external instruction is received to transfer said encrypted content data held in said first storage unit, said control unit is driven by a result of comparing second user ID data externally provided for said reproduction

apparatus with said first user ID data held in said user information hold unit, to control said second storage unit to provide said license information data to said data input/output unit.

14. (Original) The device of claim 1, further comprising a second storage unit holding license information data corresponding to said encrypted content data, respectively, and required for reproducing said encrypted content data, said license information each including content user ID data corresponding for each said encrypted content data, wherein an external instruction is received to transfer said encrypted content data held in said first storage unit, said control unit is driven by a result of comparing second user ID data externally provided for said reproduction apparatus, said first user ID data held in said user information hold unit and said content user ID data with each other, to control said second storage unit to provide said data input/output unit with said license information data for each said encrypted content data.

15. (Original) The device of claim 14, wherein said control unit is driven by a result of comparing second user ID data externally provided for said reproduction apparatus with said first user ID data held in said user information hold unit, to permit changing said content user ID data.

16. (Original) The device of claim 14, wherein said content user ID data is said first user ID data held in said user information hold unit when said encrypted content data corresponding thereto is distributed.

Amendment

Serial No. 10/069,113

Attorney Docket No. 020233

17. (Original) The device of claim 16, wherein said control unit is driven by a result of comparing second user ID data externally provided for said reproduction apparatus with said first user ID data held in said user information hold unit, to permit changing said content user ID data.

18. (Original) The device of claim 1, wherein:

said first storage unit is semiconductor memory; and

said recording device is a memory card.